ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Flexibility of the Natural Source of Attribute Based Encryption Based on the Network

[1] C.Selvalakshmi, [2] M.Karthikeyan
[1]PG Scholar, [2] HOD
[1][2]Dept. of CSE, Sengunthar College of Engineering,Tiruchengode

***Abstract* – Attribute based encryption (ABE) is a famous cryptographic generation to protect the security of users' data. However, the decryption cost and cipher text size restriction the utility of ABE in exercise. For most present ABE schemes, the decryption price and cipher text size develop linearly with the complexity of access structure. This is unwanted to the gadgets with restrained computing functionality and garage area. Outsourced decryption is taken into consideration as a possible method to lessen the consumer's decryption overhead, which allows a person to outsource a big variety of decryption operations to the cloud provider issuer (CSP). However, outsourced decryption cannot guarantee the correctness of transformation finished by means of the cloud, so it's far vital to test the correctness of outsourced decryption to make certain safety for users' facts. Current research mainly specializes in verifiability of outsourced decryption for the legal users. It nonetheless stays a hard difficulty that a way to guarantee the correctness of outsourced decryption for unauthorized users. In this paper, we recommend an ABE scheme with verifiable outsourced decryption (called full verifiability for outsourced decryption), that could simultaneously test the correctness for transformed cipher text for the authorized customers and unauthorized customers. The proposed ABE scheme with verifiable outsourced decryption is proved to be selective CPA at ease within the standard version.**

Keywords---Attribute based encryption,outsourced decyrption,CPA-secure.

1. INTRODUCTION

The development of Internet and distributed computing technology, a large amount of sensitive information is shared through computer networks or public communication facilities. Meanwhile, CSP needs to formulate flexible and scalable access control policies, and then restrict the range for data sharing. CSP also needs to ensure the confidentiality of data in the communication process with the user. In recent years, cloud computing has been rapidly developed and CSP can provide a vari-ety of services for users, such as outsourcing delegation computation and data storage, etc. A user is able to up-load a large amount of data to CSP, and share the data with other users. In addition, CSP handles a large number of data calculations according to the user's requirements, which greatly reduces the users' local computational cost. However, with the development of cloud computing, how to realize the secure storage of sensitive data is a problem that needs to be solved. Sahai and Waters first presented the concept of attribute-based encryption (ABE) to realize the confidentiality and flexible access control for encrypted data by users. For many existing ABE scheme, the pairing operations and the decryption time grow with the complexity for the access policy. For the users with resource-limited devices, it can't handle such time-consuming pairing operations or it takes a long time to decrypt. In order to reduce the computation cost and the users' decryption time, Green et al. presented an ABE scheme with outsourced de-cryption.

In this scheme, a user does not directly decrypt the original ciphertext. A untrusted server first translates the original ciphertext into a partial ciphertext with a transformation key, and then the user spends a small overhead to obtain the plaintext from the partial cipher-text. Only the users that their attributes satisfy the access policy are able to obtain the plaintext. The ABE scheme with outsourced decryption would not leak any informa-ion about the encrypted data; even the malicious CSP cannot learn anything from the ciphertext.

2. RELATED WORK

Access control in content distribution networks (CDNs) is a long-standing problem and has attracted extensive research. Traditional centralized access control approaches, such as reference monitor based approach, do not suit for CDNs as such networks are of large scale and geographically distributed in nature. Current CDNs usually resort to cryptographic-based distributed approaches for better fulfilling the goal of access control. Hence, it is highly critical to design and adapt appropriate cryptographic primitives for such purpose. We propose a novel distributed access control approach for CDNs by exploiting a new cryptographic primitive called Cipher text Policy Attributed-Based Encryption (CP-ABE). Our approach provides flexible yet fine-grained access control

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

(per file level) so that the contents are available only to the authorized users. We further consider the protection of user privacy and enhance the current design of CP-ABE so that not only the contents themselves but also the access policies, which could lead to the revelation of sensitive user information, are well protected.

Attribute-based Encryption (ABE) is regarded as a promising cryptographic conducting tool to guarantee data owner's direct control over their data in public cloud storage. The earlier ABE schemes involve only one authority to maintain the whole attribute set, which can bring a single-point bottleneck on both security and performance. Subsequently, some multi-authority schemes are proposed, in which multiple authorities separately maintain disjoint attribute subsets. However, the single-point bottleneck problem remains unsolved. In this paper, from another perspective, we conduct a threshold multi-authority CP-ABE access control scheme for public cloud storage, named TMACS, in which multiple authorities jointly manage a uniform attribute set. In TMACS, taking advantage of (t; n) threshold secret sharing, the master key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities.

Security and performance analysis results show that TMACS is not only verifiable secure when less than t authorities are compromised, but also robust when no less than t authorities are alive in the system. Furthermore, by efficiently combining the traditional multi-authority scheme with TMACS, we construct a hybrid one, which satisfies the scenario of attributes coming from different authorities as well as achieving security and system-level robustness. We present a new methodology for realizing Cipher text-Policy Attribute Encryption (CPABE) under concrete and non interactive cryptographic assumptions in the standard model. Our solutions allow any encryptor to specify access control in terms of any access formula over the attributes in the system. In our most efficient system, cipher text size, encryption, and decryption time scales linearly with the complexity of the access formula. The only previous work to achieve these parameters was limited to a proof in the generic group model. We present three constructions within our framework. Our first system is proven selectively secure under a assumption that we call the decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) assumption which can be viewed as a generalization of the BDHE assumption. Our next two constructions provide performance tradeoffs to achieve provable security respectively under the (weaker) decisional Bilinear Diffie-Hellman Exponent and decisional Bilinear Diffie-Hellman assumptions.

Public-Key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device. While this is useful for applications where the data provider knows specifically which user he wants to share with, in many applications the provider will want to share data according to some policy based on the receiving user's credentials. In cloud computing, searchable encryption scheme over outsourced data is a hot research field. However, most existing works on encrypted search over outsourced cloud data follow the model of "one size fits all" and ignore personalized search intention. Moreover, most of them support only exact keyword search, which greatly affects data usability and user experience. So how to design a searchable encryption scheme that supports personalized search and improves user search experience remains a very challenging task.
In this paper, for the first time, we study and solve the problem of personalized multi-keyword ranked search over encrypted data (PRSE) while preserving privacy in cloud computing. With the help of semantic ontology Word Net, we build a user interest model for individual user by analyzing the user's search history, and adopt a scoring mechanism to express user interest smartly. To address the limitations of the model of "one size fit all" and keyword exact search, we propose two PRSE schemes for different search intentions. Extensive experiments on real-world dataset validate our analysis and show that our proposed solution is very efficient and effective. Keyword-based search over encrypted outsourced data has become an important tool in the current cloud computing scenario. The majority of the existing techniques are focusing on multi-keyword exact match or single keyword fuzzy search. However, those existing techniques find less practical significance in real-world applications compared with the multi-keyword fuzzy search technique over encrypted data.

The first attempt to construct such a multi-keyword fuzzy search scheme was reported by Wang et al., who used locality-sensitive hashing functions and Bloom filtering to meet the goal of multi-keyword fuzzy search. Nevertheless, Wang's scheme was only effective for a one letter mistake in keyword but was not effective for other common spelling mistakes. Moreover, Wang's scheme was vulnerable to server out-of-order problems during the ranking process and did not consider the keyword weight.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

In this paper, based on Wang et al.'s scheme, we propose an efficient multi-keyword fuzzy ranked search scheme based on Wang et al.'s scheme that is able to address the aforementioned problems. we develop a new method of keyword transformation based on the uni-gram, which will simultaneously improve the accuracy and creates the ability to handle other spelling mistakes. In addition, keywords with the same root can be queried using the stemming algorithm. Furthermore, we consider the keyword weight when selecting an adequate matching file set. Experiments using real-world data show that our scheme is practically efficient and achieve high accuracy.

3. ATTRIBUTE BASED ENCRYPTION

Attribute-based encryption (ABE) is a public-key based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud, using access polices and ascribed attributes associated with private keys and cipher texts. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently, Green et al. proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. In such a system, a user provides an un trusted server, say a cloud service provider, with a transformation key that allows the cloud to translate any ABE cipher text satisfied by that user's attributes or access policy into a simple cipher text, and it only incurs a small computational overhead for the user to recover the plaintext from the transformed cipher text. Security of an ABE system with outsourced decryption ensures that an adversary (including a malicious cloud) will not be able to learn anything about the encrypted message; however, it does not guarantee the correctness of the transformation done by the cloud.

We consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. We give the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. We prove that our new scheme is both secure and verifiable, without relying on random oracles. Finally, we show an implementation of our scheme and result of performance measurements, which indicates a significant reduction on computing resources imposed on users. In distributed settings with un trusted servers, such as the cloud, many applications need mechanisms for complex access-control over encrypted data. Sahai and Waters addressed this issue by introducing the notion of attribute-based encryption (ABE). ABE is a new public key based one-to-many encryption that enables access control over encrypted data using access policies and ascribed attributes associated with private keys and cipher texts. There are two kinds of ABE schemes: key-policy ABE (KP-ABE) and cipher text-policy ABE (CP-ABE). In a CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes.

A user is able to decrypt a cipher text only if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text. In a KP-ABE scheme, the roles of an attribute set and an access policy are swapped from what we described for CP-ABE: attributes sets are used to annotate the cipher texts and access polices over these attributes are associated with users' private keys. In the following, we will use the terms access policy, access structure and access formula interchangeably. Attribute-based encryption (ABE) with outsourced decryption not only enables fine-grained sharing of encrypted data, but also overcomes the efficiency drawback (in terms of cipher text size and decryption cost) of the standard ABE schemes. In particular, an ABE scheme with outsourced decryption allows a third party (e.g., a cloud server) to transform an ABE cipher text into a (short) El Gamal-type cipher text using a public transformation key provided by a user so that the latter can be decrypted much more efficiently than the former by the user.

A shortcoming of the original outsourced ABE scheme is that the correctness of the cloud server's transformation cannot be verified by the user. That is, an end user could be cheated into accepting a wrong or maliciously transformed output. In this paper, we first formalize a security model of ABE with verifiable outsourced decryption by introducing a verification key in the output of the encryption algorithm. We present an approach to convert any ABE scheme with outsourced decryption into an ABE scheme with verifiable outsourced decryption. The new approach is simple, general, and almost optimal. Compared with the original outsourced ABE, our verifiable outsourced ABE neither increases the user's and the cloud server's computation costs except some non dominant operations (e.g., hash computations), nor expands the cipher text size except adding a hash value

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

We show a concrete construction based on Green et al.'s cipher text-policy ABE scheme with outsourced decryption, and provide a detailed performance evaluation to demonstrate the advantages of our approach.

Traditionally, access controls to data operate on the assumption that data servers can be trusted to keep data confidential and enforce access control policies correctly. However, this assumption is no longer true today since services are increasingly storing data across many servers that are shared with other data owners. An example of this is cloud data storage where cloud service providers are not in the same trusted domains as end users, and hardware platforms are not under the direct control of data owners. To mitigate users' privacy concerns about their data, a common solution is to store data in encrypted form so that it will remain private, even if data servers or storage devices are not trusted or compromised. The encrypted data, however, must be amenable to sharing and access control.

Attribute-based encryption (ABE) provides a mechanism for complex access control over encrypted data. However in most ABE systems, the cipher text size and the decryption overhead, which grow with the complexity of the access policy, are becoming critical barriers in applications running on resource-limited devices. Outsourcing decryption of ABE cipher texts to a powerful third party is a reasonable manner to solve this problem. Since the third party is usually believed to be un trusted, the security requirements of ABE with outsourced decryption should include privacy and verifiability. Namely, any adversary including the third party should learn nothing about the encrypted message, and the correctness of the outsourced decryption is supposed to be verified efficiently. We propose generic constructions of CPA-secure and RCCA-secure ABE systems with verifiable outsourced decryption from CPA-secure ABE with outsourced decryption, respectively. We also instantiate our CPA-secure construction in the standard model and then show an implementation of this instantiation. The experimental results show that, compared with the existing scheme, our CPA-secure construction has more compact cipher text and less computational costs. Moreover, the techniques involved in the RCCA-secure construction can be applied in generally constructing CCA-secure ABE, which we believe to be of independent interest.

Attribute-Based Encryption (ABE) is a promising cryptographic primitive which significantly enhances the versatility of access control mechanisms. Due to the high expressiveness of ABE policies, the computational complexities of ABE key-issuing (by Attribute Authorities (AAs)) and decryption (by eligible users) are getting prohibitively high. Despite that the existing Outsourced ABE solutions are able to offload some intensive computing tasks to a third party, for example, a cloud, so to relieve the local burden of eligible users during decryption, the high computational complexity of the key-issuing at the AAs has yet to be addressed, while an ABE system will continue to grow with more users being included, and with the user revocation being considered in practice which will trigger more key (re-)issuing. Aiming at tackling the challenges above, for the first time, we propose a Secure Outsourced ABE system, which not only supports secure outsourced decryption, but also provides secure outsourced key-issuing. Unlike the current outsourced ABE systems, our new method offloads all access policy and attribute related operations in the key-issuing process or decryption to a Key Generation Service Provider (KGSP) and a Decryption Service Provider (DSP), respectively, leaving only a constant number of simple operations for the AAs and eligible users to perform locally. Furthermore, we show that both outsourcing processes (to KGSP and to DSP) are secure, namely, the KGSP and the DSP would not be able to recover the keys or decrypt the cipher texts, respectively. In addition, we consider the scenario that a KGSP or DSP may be dishonest and could maliciously generate some incorrect returning values rather than following the outsourced operations. Therefore, in this paper, we also propose another ABE construction which allows the AAs and eligible users to check the correctness of outsourced operations in an efficient way. The security of the construction is analyzed under a recently formalized model called Refereed Delegation of Computation (RDoC).

Attribute-Based Encryption (ABE) has attracted much attention in the research community. In ABE system, users' private keys and cipher texts are labeled with sets of descriptive attributes and access policies respectively, and a particular key can decrypt a particular cipher text only if associated attributes and policy are matched. Until now, there are two kinds of ABE having been proposed: Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher text-Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, the access policy is assigned in private key, whereas, in CP-ABE, it is specified in cipher text. Recently, as the development of cloud computing, users' concerns about data security are the main obstacles

ISSN (Online) 2394-2320

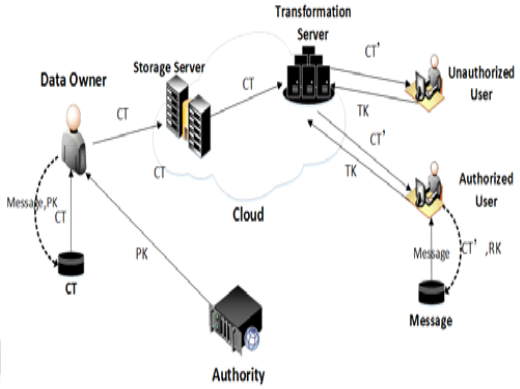
International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

that impedes cloud computing from widely adopted. These concerns are originated from the fact that sensitive data resides in public cloud, which is maintained and operated by untrusted Cloud Service Provider (CSP). ABE provides a secure way that allows data owner to share outsourced data on untrusted storage server instead of trusted server with specified group of users. This advantage makes the methodology appealing in cloud storage that requires secure access control for a large number of users belonging to different organizations.

Some of the most challenging issues in data outsourcing scenario are the enforcement of authorization policies and the support of policy updates. Cipher text-policy attribute-based encryption is a promising cryptographic solution to these issues for enforcing access control policies defined by a data owner on outsourced data. However, the problem of applying the attribute-based encryption in an outsourced architecture introduces several challenges with regard to the attribute and user revocation. We propose an access control mechanism using cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation capability. The fine-grained access control can be achieved by dual encryption mechanism which takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. We demonstrate how to apply the proposed mechanism to securely manage the outsourced data. The analysis results indicate that the proposed scheme is efficient and secure in the data outsourcing systems. Modern data outsourcing systems require flexible access control approaches. In many cases, it is desirable to provide differentiated access services such that data access policies are defined over user attributes or roles. The data outsourcing scenario challenges the approaches of traditional access control architectures such as reference monitor, where a trusted server is in charge of defining and enforcing access control policies. This assumption no longer holds in modern data our sourcing systems, because users want to be able to share private contents with a group of people they selected and to define some access policy and enforce it on the contents. Thus, it is desirable to put the access policy decisions in the hands of the data owners.

4. CP-ABE FULLY VERIFY OUTSOURCED DECRYPTION

Proposed ABE scheme with verifiable outsourced decryption is proved to be selective CPA-secure in the standard model. First proposed KP-ABE for fine-grained access control of encrypted data. Proposed the first CP-ABE scheme, which is more suitable for practical application requirements. Proposed a privacy-preserving decentralized CP-ABE scheme with fully hidden access structure, which has been applied in personal health record.



This technique is Clearly an adversary who can eavesdrop on a password authentication can then authenticate itself in the same way. One solution is to issue multiple passwords, each of them marked with an identifier. The verifier can ask for any of the passwords, and the prover must have that correct password for that identifier.

Assuming that the passwords are chosen independently, an adversary who intercepts one challenge-response message pair has no clues to help with a different challenge at a different time. For example, when other communications security methods are unavailable, the U.S. military uses the AKAC-1553 TRIAD numeral cipher to authenticate and encrypt some communications. TRIAD includes a list of three-letter challenge codes, which the verifier is supposed to choose randomly from, and random three-letter responses to them. For added security, each set of codes is only valid for a particular time period which is ordinarily 24 hours.

A more interesting challenge-response technique works as follows: Say "Bob" is controlling access to some resource. Alice comes along seeking entry. Bob issues a challenge, perhaps "52w72y". Alice must respond with the one string of characters which "fits" the challenge Bob issued. The "fit" is determined by an algorithm "known" to Bob and Alice. (The correct response might be as simple as "63x83z" (each character of response one more than that of challenge), but in the real world, the "rules" would be much more complex.) Bob issues a different challenge each time, and thus knowing a previous correct response (even if it isn't "hidden" by the means of communication

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

used between Alice and Bob) is of no use. A part of Alice's response might convey that it is Alice who is seeking authentication.

Definitions

Definition 1 (Access Structure [4]) Let {P1, P2, . . . , Pn} be a set of parties. A collection A ⊆ 2 {P1,P2,...,Pn} is monotone if ∀B, C : if B ∈ A and B ⊆ C then C ∈ A. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of {P1, P2, . . . , Pn}, i.e., A ⊆ 2 {P1,P2,...,Pn}\{∅}. The sets in A are called the authorized sets, and the sets not in A are called the unauthorized sets. In our context, the role of the parties is taken by the attributes. Thus, the access structure A will contain the authorized sets of attributes. We restrict our attention to monotone access structures. However, it is also possible to (inefficiently) realize general access structures using our techniques by having the not of an attribute as a separate attribute altogether. Thus, the number of attributes in the system will be doubled. From now on, unless stated otherwise, by an access structure we mean a monotone access structure. An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms. Setup This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK. Encryption This is a randomized algorithm that takes as input a message m, a set of attributes γ, and the public parameters PK. It outputs the ciphertext E. Key Generation This is a randomized algorithm that takes as input – an access structure A, the master key MK and the public parameters PK. It outputs a decryption key D. Decryption This algorithm takes as input – the ciphertext E that was encrypted under the set γ of attributes, the decryption key D for access control structure A and the public parameters PK. It outputs the message M if γ ∈ A.

Definition 2 An attribute-based encryption scheme is secure in the Selective-Set model of security if all polynomial time adversaries have at most a negligible advantage in the Selective-Set game.

Bilinear Maps We present a few facts related to groups with efficiently computable bilinear maps. Let G1 and G2 be two multiplicative cyclic groups of prime order p. Let g be a generator of G1 and e be a bilinear map, e : G1 × G1 → G2. The bilinear map e has the following properties:

1. Bilinearity: for all u, v ∈ G1 and a, b ∈ Zp, we have e(u a , vb) = e(u, v) ab .

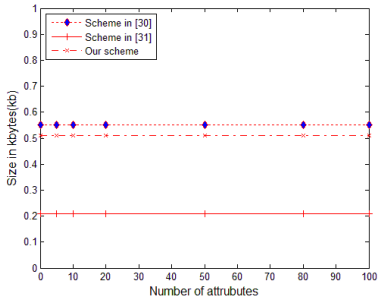
2. Non-degeneracy: e(g, g) 6= 1. We say that G1 is a bilinear group if the group operation in G1 and the bilinear map e : G1 × G1 → G2 are both efficiently computable. Notice that the map e is symmetric since e(g a , gb) = e(g, g) ab = e(g b , ga).

The Decisional Bilinear Diffie-Hellman (BDH) Assumption Let a, b, c, z ∈ Zp be chosen at random and g be a generator of G1. The decisional BDH assumption is that no probabilistic polynomial-time algorithm B can distinguish the tuple (A = g a , B = g b , C = g c , e(g, g) abc) from the tuple (A = g a , B = g b , C = g c , e(g, g) z) with more than a negligible advantage. The advantage of B is ¯ ¯ ¯Pr[B(A, B, C, e(g, g) abc) = 0] − Pr[B(A, B, C, e(g, g) z)] = 0 ¯ ¯ ¯ where the probability is taken over the random choice of the generator g, the random choice of a, b, c, z in Zp, and the random bits consumed by B.

5. OUTSOURCED ABE DECRYPTION

If an outsourced ABE with verification does not have a verification key (i.e., VK = ∅), we refer to it as the standard notion of outsourced ABE (without verification) [8]. We denote by ABEO = (Setup,Encrypt,KeyGen, Transform, Decrypt) an outsourced ABE system. In Section IV, the outsourced ABE essentially works in the KEM setting, where the ABE ciphertext hides a symmetric session key. The formal definition of attribute-based KEM with outsourced decryption is exactly the same as that of ABE with outsourced decryption, except that the encryption algorithm of ABE is replaced by an encapsulation algorithm, which doesn't take a message as an input. We show that any outsourced ABE system can be simply converted to an attribute-based KEM with outsourced decryption via the following method: the encapsulation algorithm takes as input MPK and Ienc. It first chooses a random session key (message) K from M, and then computes CTIenc ← Encrypt(MPK, K, Ienc) using the encryption algorithm of the outsourced ABE. Finally, it outputs (CTIenc , K).

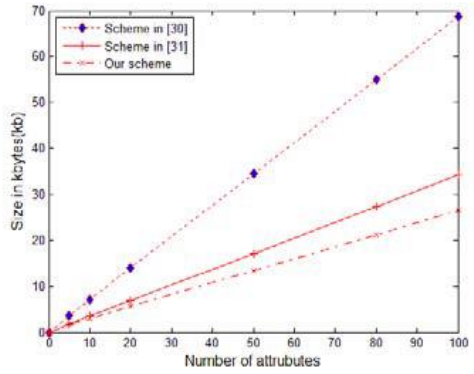
Normal ABE chipertext size



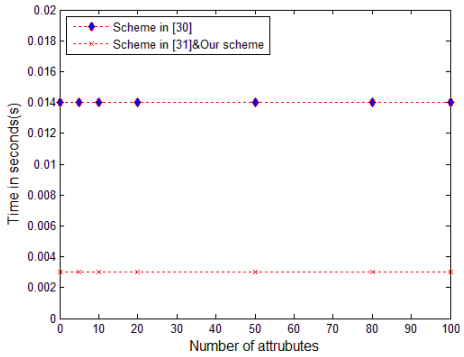
ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Partial decrypted chipertext size



Decryption time



6. CONCLUSION

We present a full verifiability for out-sourced decryption in ABE. In our construction, there are two kinds of users can verify the correctness of the outsourced transformed ciphertext. One is the authorized user who can verify the correctness for the transformed ciphertext and decrypt the ciphertext to obtain the original message. Another is the unauthor-ized user who has the ability to verify the correctness of the transformed ciphertext, but he does not decrypt the ciphertext to obtain the original message. We prove the proposed scheme is selective CPA-secure in standard model. Compared with schemes our scheme is more efficient.

REFERENCES

1. A. Sahai, B. Waters, "Fuzzy identity based encryption," Proc. EU-ROCRYPT 2005, LNCS 3494, Springer, pp. 457–473, 2005.
2. V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM conference on Computer and Communications Security, pp. 89-98, 2006.
3. J. Bethencourt, A. Sahai and B. Waters, "Cipher text-policy attribute-based encryption," Proc. IEEE Symposium on Security and Privacy, pp. 321-334, 2007.
4. B. Waters, "Cipher text-policy attribute-based encryption: an expressive, efficient, and provably secure realization," in Public Key Cryptog-raphy (PKC '11), pp. 53-70, 2011.
5. L. Cheung and C. Newport, "Provably secure cipher text policy ABE," Proc. 14th ACM conference on Computer and Communications Security, pp. 456-465, 2007.
6. L. Inraimi, Q. Tang, P. Hartel and W. Jonker, "Efficient and provable secure cipher text-policy attribute-based encryption schemes," Proc. ISPEC 2009, LNCS 5451, Springer, pp. 1-12, 2009.
7. S. Yu, K. Ren and W. Lou, "Attribute-based content distribution with hidden policy," Proc. IEEE 4th Workshop on Secure Network Protocols, pp. 39-44, 2008.
8. F. K, A.M J and J. Li, "Attribute-based access control with hidden policies and hidden credentials," IEEE Trans. Computers, vol. 55, no. 10 pp. 1259-1270, 2006, doi:10.1109/TC.2006.158.
9. J. Lai, R.H. Deng and Y. Li, "Expressive CP-ABE with partially hidden access structures," Proc. 7th ACM Symposium on Information, Computer and Communications Security, pp. 18-19, 2012.
10. M. Chase and S.S.M. Chow, "Improving privacy and security in multi-authority attribute-based encryption," Proc.14th ACM conference on Computer and Communications Security, pp. 121-130, 2009.
11. W. Li, K. Xue, Y. Xue and J. Hong, "TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Trans. Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484-1496, 2015.
12. J. Li, X. Huang, J.W. Li, X. Chen and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability," IEEE Trans. Parallel and Distributed Systems, vol. 25, no. 8, pp. 2201-2210, 2014.
13. J. Hur and D. K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Transactions on Parallel and Distributed Systems, pp. 1214-1221, 2011.
14. X. Mao, J. Lai, Q. Mei, K. Chen and J. Weng, "Generic and efficient constructions of attribute-based

encryption with verifiable outsourced decryption," IEEE Trans. Dependable and Secure Computing, 2015.
15. S. Lin, R. Zhang, H. Ma and M. Wang, "Revisiting attribute-based encryption with efficient verifiable outsourced decryption," IEEE Trans. Information Forensics and Security, vol. 10, no. 10, pp. 2119-2130, 2015.
16. J. Li, F. Sha, Y. Zhang, X. Huang, and J. Shen, "Verifiable Out-sourced Decryption of Attribute-Based Encryption with Con-stant Ciphertext Length," Security and Communication Networks, 2017, doi:10.1155/2017/3596205.
17. Y. Hu and H. Jia, "Cryptanalysis of GGH Map," Proc. EUROCRYPT 2016, LNCS 9665, Springer, pp. 537–565, 2016.
18. Z. J. Fu, K. Ren, J. G. Shu, X. M. Sun, and F. X. Huang, "Ena-bling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel and Distributed Systems, , vol. 27, no. 9, pp. 2546–2559, 2016.
19. Z. Fu, X. Wu, C. Guan, X. Sun and K. Ren, "Towards Efficient Multi-keyword Fuzzy Search over Encrypted Outsourced Da-ta with Accuracy Improvement," IEEE Transactions on Informa-tion Forensics and Security, vol. 11, no. 12, pp. 2706-2716, 2016.
20. J. Li, H. Wang, Y. Zhang and J. Shen, "Ciphertext-policy at-tribute-based encryption with hidden access policy and test-ing, " KSII Transactions on Internet and Information Systems, vol. 10, no. 7, pp. 3339-3352, 2016.